

SIATS Journals

Journal of Human Development and Education for specialized Research

(JHDESR)

Journal home page: http://www.siats.co.uk



مجلة التنمية البشرية والتعليم للأبحاث التخصصية

العدد 4، المجلد 4 ، أكتوبر 2018م.

e ISSN 2462–1730

THE USE OF BIOMETRICS IN INFORMATIVE INSTITUTIONS: ACADEMIC LIBRARIES AS AN EXAMPLE

Dr.Maha A.Ibrahim

mahaahmed_2003@yahoo.com

Associate Professor of Information Science Department

Faculty of Arts-Beni-Suef University

1439هـ –2018م

ARTICLE INFO
Article history:
Received 01/06/2018
Received in revised form 25/06/2018
Accepted 21/09/2018
Available online 15/10/2018
Keywords: Biometrics, Biometrics In library and Information sciences, Biometrics in Academic Libraries.

Abstract

This study aims to identify the possibility of the use of biometrics in library and information Profession, especially in the Academic libraries because they seek to provide advanced services to meet all the needs of researchers from the faculty and student members at all levels, has been the use of the curriculum descriptive analytical and review the concept of biometrics and the categories and areas that account for using biometrics applications and to shed light on the use of biometrics in the field of Academic Libraries and the advantages that accrue to libraries to use those applications as well as the flaws and the problems they face, as well as make recommendations which they can use those measurements effectively in Academic Libraries.

Key Words: Biometrics, Biometrics In library and Information sciences, Biometrics in Academic Libraries.

Introduction:

Modern advanced technologies have played an essential part in communication sciences. They led individuals to live in a visual society where the old coined term 'Hypotheticsociety 'is not much appreciated ; it become a common and widespread term among all users of the internet. In this respect, biometrics, as a science, can be defined here as "a science of measuring both physiological and behavioral characteristics that can identity accurately the identity of the individual. Biometric identification technology adopts graphical information can be scanned from the image of face, retina, fingerprint shape, voice pattern, facial recognition, and identification of hand geometry" (1) to identify the types of biometrics and the possibility of using biometrics in informative institutions like Academic Libraries.

Most importantly, the study seeks to identify biometrics and its applications inAcademic Libraries as a source of sciences and knowledge for all researchers and students all over the world. Biometrics is used in information security since the early dawn, but at these days, they are used in

libraries. Thus, the present study highlights the importance of using biometrics in libraries andAcademic Libraries.

Biometric technologies offer one of the most promising approaches to providing user friendly and reliable control methodology for access to computer systems, networks and workplaces. They aimed at "studying well established physical biometrics such as fingerprint or iris recognition. Behavioral biometrics are usually only briefly mentioned and only those which are in large part based on muscle control such as keystrokes, gait or signature are well investigated"([2]).

Scientific research is considered an essential part of any progressed society. Hence, the researcheris a major pillar of thescientific research for his contribution in pushing the wheel of progress and development of the scientific research. Furthermore, university library is cornerstone in the educational process and scientific research. These libraries are not away from the world, but they must strive towards providing advanced services to meet all the needs of researchers on a large scale.

Descriptive analytic approach is adopted in the present study as an approach to achieve the study aims, and to highlight biometrics' use in Academic Libraries.

Review of Literature

It is clear that a considerable number of scholars have tackled biometrics from different aspects rather than focusing on their use in libraries. One these studiesis:

"Our Biometric Future: The Social Construction of an Emerging Information Technology " is a Ph.D. thesis submitted by Gates, Kelly Allison,University of Illinois at Urbana-Champaign, 2004.This thesisexamines the social construction of facial recognition, a unique and technically challenging type of biometric,from early research and development in the 1960s to its incorporation into the US-VISIT automated entry/exit system mandated by post-9/11 U.S. federal policy. The methodology combines cultural analysis, political economy, and the social construction of technology (SCOT) approach, drawing from scientific articles, press accounts, U.S. government documents, company web sites and publicity materials, conference proceedings, popular culture texts, interviews with individuals involved in biometric research and implementation, participant observation at industry conferences, and a site visit to Tampa, Florida to observe a biometric system in operation. The evidence suggests that the emergence of these new

access control technologies is an integral dimension of the transition to what Dan Schiller calls "informationalized capitalism" ([i]).

"Ocular biometrics: Human Recognition in Challenging Conditions"is a Ph.D. thesis submitted by Global Forkin, M (2011), University ofWake Forest. It proposes a definition for the term ocular region and shows how recognition performance using this region is more robust under challenging imaging conditions. It also presents new approaches to ocular recognition that outperform iris recognition on challenging datasets, thus providing strong justification and motivation for further study of the ocular region as a biometric. These methods include an optimized scale invariant feature transform (SIFT) and a fusion method utilizing SIFT and Gabor filter encoding (ii).

"Biometrics Technology: Understanding Dynamics Influencing Adoption for Control of Identification Deception within Nigeria" is a Ph.D. Thesis submitted by Nwatu, G. U. (2011). The objective of the study was to provide scholarly research about the factors that influenced the adoption of biometrics technology to reliably identify and verify individuals in Nigeria to control identity fraud. The mixed-method descriptive and inferential study used interview and survey questionnaires for data collection. The implications for social change include leveraging biometrics technology for recognition, confirmation, and accountability of individuals to prevent identity scheming, ensure security, and control the propagation of personal information. Beyond these immediate benefits, this research presents an example that other developing countries may use to facilitate the adoption of biometrics technology.(iii)

"Intrusion detection using spatial information and behavioral biometrics" is a Ph.D. Thesis submitted by Yampolskiy, R. V. (2008) in The University of State University of New York at Buffalo Buffalo. This dissertation begins with a review of published research in game security and behavioral biometrics. We analyze previous studies and point out trends and propose taxonomies which make understanding and improvement on previous work easier. As the capstone of this dissertation, we have developed an intrusion detection system for online poker which uses player's game strategy as the behavioral profile. We have improved our system by experimenting with different similarity measure functions and different ways of representing behavioral signatures. As the research progressed new interesting and unforeseen research paths were discovered. We have expanded strategy-based behavioral biometrics to a new domain of recognition and verification of

intelligent agents and had created a novel CAPTCHA-based algorithm aimed at preventing intelligent agents from participating in online poker games (iv).

"A statistical approach towards performance analysis of multimodal biometric systems" is a Ph.D. Thesis submitted by Xiaobu Yuan and Wei Gan (2008).This thesis investigates the application of statistical methods in performance analysis of multimodal biometric systems. It develops an efficient and systematic approach to evaluate system performance in different situations of noise influences. Using this approach, 126 experiments are conducted with the BSSR1 dataset. The proposed approach helps to examine the performance of typical fusion methods that use different normalization and data partitioning techniques (v).

“An empirical investigationof tree ensembles in biometrics and bioinformatics research” is a Ph.D. thesis submitted by Ma, Y. (2007). This thesis explores the usability and efficiency of tree ensemble learning when applied to the following research areas: multi-modal biometrics information fusion, software defect prediction and microarray data analysis. The data sets from these three areas have various structures in terms of the sample size, number of features, and the class labels distribution. For example, microarray experiments produce high-dimensional data with at least thousands of variables (genes), while the data sets from biometrics and software engineering studies are large-sized with hundreds to thousands of observations, majority of which are of the same class label. Different data structure has certain requirements on the learning algorithms. No matter what requirements are posedon the learning techniques, the ultimate goal is to achieve a high prediction accuracy as much as possible. This thesis centers on making the best use of tree ensemble learning methodologies in biometrics, software engineering and microarray research (vi).

"Thermal imaging as a biometrics approach to facial signature authentication" is a Ph.D. This is submitted by Guzman Tamayo, A. M. (2011).in The University of Florida International. This dissertation develops an image processing framework with unique feature extraction and similarity measurements for human face recognition in the thermal mid-wave infrared portion of the electromagnetic spectrum. The goals of this research is to design specialized algorithms that would extract facial vasculature information, create a thermal facial signature and identify the individual. The objective is to use such findings in support of a biometrics system for human identification with a high degree of accuracy and a high degree of reliability. The proposed thermal

facial signature recognition is fully integrated and consolidates the main and critical steps of feature extraction, registration, matching through similarity measures, and validation through testing our algorithm on a database, referred to as C-X1, provided by the Computer Vision Research Laboratory at the University of Notre Dame.

The highly accurate results obtained in the matching process along with the generalized design process clearly demonstrate the ability of the thermal infrared system to be used on other thermal imaging based systems and related databases. A novel user-initialization registration of thermal facial images has been successfully implemented. Furthermore, the novel approach at developing a thermal signature template using four images taken at various times ensured that unforeseen changes in the vasculature did not affect the biometric matching process as it relied on consistent thermal features(vii).

HOMOGENEOUS COGNITIVE BASED BIOMETRICS FOR STATIC AUTHENTICATION is a Ph.D. Thesis submitted by OmarHamdyMohamed (2010). In this research, it was proposed a novel biometric system for static user authentication that homogeneously combines mouse dynamics, visual search capability and short-term memory effect. The proposed system introduces the visual search capability, and short-term memory effect to the biometric-based security world for the first time. The use of mouse for its dynamics, and as an input sensor for the other two biometrics, means no additional hardware is required. Experimental evaluation demonstrated the system's effectiveness using variable or one-time passwords. All of these attributes qualify the proposed system to be effectively deployed as a static Web-authentication mechanism.

Extensive experimentation was done using 2740 sessions collected from 274 users. Two classification mechanisms were used to measure the performance. Using the first of these, a specially devised neural network model called Divide &Select, an EER of 5.7% was achieved. A computational statistics model showed a higher classification performance; a statistical classifier design called Weighted-Sum produced an EER of 2.1%.

The performance enhancement produced as a result of changing the analysis model suggests that with further analysis, performance could be enhanced to an industry standard level. Additionally, we presented a Proof of Concept (POC) system to show the system packaging practicality (viii).

Situational considerations in information security: Factors influencing perceived invasiveness toward biometrics" is a Ph.D. Thesis submitted by Brydie, Daryl Richard, (2009) in The University of CAPELLA .This exploratory study provides a platform for extending the body of knowledge associated with the nature of perceived invasiveness toward biometric technologies. This analysis of perceived invasiveness was conducted via consideration of situational factors which may influence an individual's willingness to use such technologies. Specifically, this research validated a proposed conceptual model and tested hypotheses which evaluated if the eye was viewed as a significantly more sensitive or invasive area of the person than the hand when subject to appraisal by biometric devices. The primary outcome of the study indicated that, within the air travel security instance, the factors of use context, preference, and proxemic sensitivity are correlated with an individual's perceived invasiveness toward eye-based biometric technologies. Consequently, only the factor of proxemic sensitivity was indicated to be correlated with individual sentiment of perceived invasiveness toward biometric technologies, regardless of the class of biometric technology under consideration.(ix).

"A High Capacity Reversible Multiple Watermarking Scheme - Applications to Images, Medical Data, and Biometrics" is a M.D. Thesis submitted by BehrangMehrbanyIrany (2011) in The University of Toronto.

The focus of this thesis is digital watermarking as a part of Digital Rights Management (DRM), security and privacy, as well as the ability to employ electrocardiogram (ECG) as a method to enhance the security and privacy level. The contribution of this work consists of two main parts: An application-specific high-capacity reversible multiple watermarking scheme is introduced in the first part to mainly target the medical images. The proposed data hiding method is designed such that the embedding of sensitive personal information in a generic image without any loss of either the embedded or the host information is possible. Furthermore, in the second part, the use of ECG biometric signals in the form of the embedded watermark is studied. Proposed framework allows embedding of ECG features into the host image while retaining the quality of the image, the performance of the security system and the privacy of the identity. Experimental results indicate that the reversible data hiding scheme outperforms other approaches in the literature in terms of payload capacity and marked image quality. Results from the ECG mark embedding also show that no major degradation in performance is noticeable compared to the case where no watermarking is needed(x).

"Toward secure, trusted, and privacy-enhanced biometrics in the cloud " is a Ph.D. Thesis submitted by Albahdal, Abdullah Abdulaziz(2015). in The University of Colorado.The primary goal of this research is to explore how biometrics can be deployed in the cloud and how the strong authentication property of biometrics can be leveraged to improve the security of the cloud, taking into account the challenges faced when using biometrics for remote applications. These challenges include the security of biometric templates, the privacy of users, and the trust for remote biometric operations. The contributions of the dissertation start with an empirical motivational study of the usability and security of passwords as the most commonly used authentication method in the cloud as compared with the privacy-enhanced fingerprint authentication. The dissertation continues by addressing the privacy and trust problems of exchanging biometric data by enhancing the Bio cryptographic Key Infrastructure (BKI) to be used as a building block for following proposed methods. The dissertation continues by proposing the trusted and privacy-enhanced biometric web identities, or Trusted-BWI. Trusted-BWI illustrates how biometric systems can be deployed in the cloud in a secure, trusted, and privacy-enhanced manner. Then, as cloud services rely heavily on the Secure Socket Layer (SSL) for network security, we propose the Bio cryptographic Secure Socket Layer (BSSL), which leverages the strong authentication property of biometrics to enhance the security and usability of the client-side authentication of SSL(11).

From the above, as it is mentioned, it becomes clear that such studies paid attention to the study of biometric in libraries on particular and Academic Libraries on general like using 'fingerprint and face detection' as an access to these libraries. The previous studies also traced privacy and security systems of the developmental countries. In this case, the present study focuses on the use of biometrics in Academic Libraries.

Definition of biometrics

Biometrics, as a term, comes from the Greeks. The combination of the words bio meaning life and metric meaning to measure makes biometry.([xi])This indicates that biometrics can be divided into:

The term "biometrics" is derived from the Greek words bio (life) and metric (to measure). *f* For our use([xii])Biometrics refers to technologies for measuring and analyzing a person's physiological or behavioral characteristics. These characteristics are unique to individuals hence can be used to verify or identify a person([xiii])

For Norman Desmarais presents biometricsis based on the principle that everyone has unique physical attributes that, in theory, a computer can be programmed to recognize. Biometrics uses mathematical representations of those unique physical characteristics to identify an individual or to verify identity. It can serve to authenticate people because everyone has unique and somewhat stable body features and ways of doing things. While passwords, cards, personal identification numbers, and keys can be forgotten, stolen, forged, lost, or given away, biology cannot be. We have all seen biometric devices used in science fiction movies. Now, they are making their way to the desktop and to personal workstations.([xiv])

Because Biometrics are designed to generate digital readings of the body as a means of identifying individuals, enlisting a number of communication technologies, including photography, video, and computer hardware and software. Applications include criminal identification, border control, building and computer security([xv]).

While both Ravinder Singh Gulairand KaranShethshow that biometrics refers to the automatic identification of a person based on his/her physiological or behavioral characteristics. They are of interest in any area where it is important to verify the true identity of an individual. This method of identification is preferred over traditional methods involving passwords and personal identification numbers (PIN) numbers. Initially, these techniques were employed primarily in specialist high security applications (xvi).

Biometric technologies are defined as automated methods of identifying or verifying the identity of a living person based on physiological or behavioral characteristics. Recently, this was modified to include chemical attributes (DNA) Nov. 2003(xvii).

Biometrics refers to technologies for measuring and analyzing a person's physiological or behavioral characteristics.

Thus, biometrics is classified into two categories: physiological and behavioral.

Physical Biometrics

- ✓ Fingerprint Identification or Recognition
- ✓ Speaker or Voice Authentication
- ✓ Hand geometry recognition
- ✓ Hand or Finger Geometry Recognition

- ✓ Facial Recognition

Behavioral Biometrics

- ✓ Keystroke or Typing Recognition
- ✓ Speaker Identification or Recognition(xviii)

All of these features are unique and they are found among persoons. Common physiological biometrics include finger (fingertip, thumb, finger length or pattern), palm (print or topography), hand geometry, wrist vein, face, and eye (retina or iris). Behavioral biometrics include voiceprints, keystroke dynamics, and handwritten signatures([xix])(xx)(xxi)([xxii])(xxiii).

For the definition of biometrics of libraries and information centres , ODLIS defines biometrics as a method of authenticating personal identity electronically through the use of digital data (usually encrypted) in which measurements of the person's unique physiological or behavioral characteristics (fingerprint, eye retina or iris print, voice or facial pattern, signature, etc.) are recorded. Some libraries use biometric scanners to identify patrons accessing the Internet via public workstations, to prevent them from logging on with the library card number or PIN code of a friend or relative. Several European countries are considering mandatory biometric ID cards for their citizens(xxiv).

A good definition of Biometrics is “The study of measurable biological characteristics. In computer security, biometrics refers to authentication techniques that rely on measurable physical characteristics that can be automatically checked.”(xxv)

Biometrics refers to technologies used to detect and recognize human physical characteristics. In the IT world, biometrics is often synonymous with "biometric authentication," a type of security authorization based on biometric input.There are several types of biometric authentication. Common examples include fingerprint scanning, retinal scanning, facial recognition, and voice analysis. A facial recognition system, for instance, uses a camera to capture an image of a person's face. The photograph is then recorded and processed using biometrics software. The software attempts to match the scanned image with an image from a database of users' photos. If the scan is close enough to a specific user, the person will receive authorization to continue.In many cases, a biometric scan is similar to a login. For example, some computers have a finger scanner that allows you to authenticate yourself by swiping your finger across a sensor. Instead of entering a username and password, the finger scan provides your authorization.

Some retail outlets now use finger scanners to verify people's identity as an alternative to entering a unique pin number. High-security government and office buildings may even require retinal scans in order to access certain areas of the building. In some cases, a keycard, passcode, or login is required in addition to a biometric scan in order to provide extra security(xxvi).

From the above definitions of biometrics in libraries focus on such techniques and tools that are used to be adopted. All definitions includes:

-Physical characteristics

- Behavioral characteristics

- Identity identification

- More effective than passwords and ID numbers

- Use of secured digital data

History of biometrics

The following is a short historical background of biometrics. Biometrics based on intrinsic physical or behavior traits goes back thousands of years. (xxvii)

The first ideas of biometrics appeared many years ago. In general, it is very difficult to say that biometrics appeared it this place at this time. The ideas to use parts of human body and even the ways to use this ideas appeared all over the world. First evidences of biometrics appeared in 29.000BC when the cavemen used their fingerprints to sign their drawings(xxviii).

Furthermore, the first known example of biometrics in practice was a form of finger printing being used in China in the 14th century, as reported by explorer Joao de Barros. He wrote that the Chinese merchants were stamping children's palm prints and footprints on paper with ink to distinguish the young children from one another. This is one of the earliest known cases of biometrics in use and is still being used today(xxix).

There are such uses of biometrics like fingerprints. They were used on clay tablets during Babylonian business transactions in 500 BC. Fourteenth century Chinese merchants used children’s palms and footprints to distinguish them. And in early Egyptian history, traders were differentiated by their physical characteristics(xxx).

In 1968, Biometrics is used in either commercial dealings or detecting terrorists and criminals. They have existed in commercially available products for a long time.

The oldest ongoing general application of biometrics belongs to the University of Georgiawhich, in 1973, installed a hand-scanning system to restrict entry into its dining halls. The device measured the lengths of members' fingers by scanning them with photoelectric cells. It is in the last decade that biometric applications have finally caught up with the technology that has been around for nearly 30 years. Biometric vendors feel that time and attendance is the biggest growth area for biometrics in the near future. Beyond time and attendance, computer and electronic commerce security offer the greatest promise for widespread biometric use. During 1990's, fingerprint identification systems were the most popular and widely used from of biometric technology. But, today, a wide variety of biometric devices such as hand scans, voice recognition system, hand geometry system, eye-scanning system, and face recognition system are available in the market.

The technological developments paved the way for the declining prices and the escalating fraud and security breeches are bringing biometric technology to market. For example, the Finance Minister of Government of India recently announced that the Income Tax Department will issue Biometric PANcards to all Tax payers([xxxi])

Applications of Biometrics:

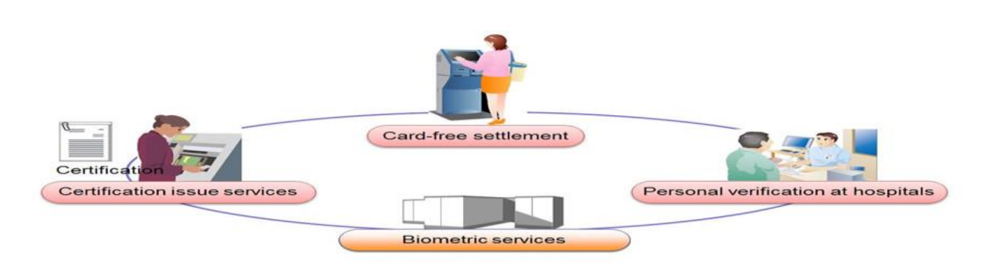
In the last few years, Biometrics have considerably increased the area of application of biometrics and it's expected that in the near future, we will use biometry many times in our daily activities such as getting in the car, opening the door of our house, accessing to our bank account, shopping by internet, accessing to our PDA, mobile phone, laptops, etc(xxxii).

Biometrics is now being used in almost every area. Not only that, but various types of biometric systems are being used to achieve various functionalities(xxxiii). Applications of biometrics can be categorized in the following five main groups: forensic, government, commercial, health-care and traveling and immigration. However, some applications are common to these groups such as physical access, PC/network access, time and attendance (34).

Applications of Biometrics can be divided into three categories:

Commercial applications, such as computer network logins, electronic data security, e-commerce, Internet access, ATMs, credit cards, physical access control, cellular phones, PDAs,

medical records management, and distance learning; government applications such as national ID cards, correctional facilities, driver's licenses, social security, border control, passport control, and welfare-disbursement; and • forensic applications such as corpse identification, criminal investigation, terrorist identification, parenthood determination, and missing children(xxxiv).



Application scenarios for large-scale biometric authentication services([xxxv]) In the following, we propose the five major applications briefly:

Forensic

The use of biometric in the law enforcement and forensic is more known and from long date, it is used mainly for identification of criminals. In particular, the AFIS (automatic fingerprint identification system) has been used for this purpose. Lately the facial-scan technology (mug shots) is being also used for identification of suspects. Another possible application is the verification of persons of home arrest, a voice-scan is an attractive solution for this problem. The typical application are: Identification of criminals ,Surveillance ,Corrections , Probation and home arrest

Government

There are many application of the biometry in the government sector. An AFIS is the primary system used for locating duplicates enrolls in benefits systems, electronic voting for local or national elections, driver's license emission, etc. The typical application are:National Identification Cards , Voter ID and Elections ,Driver's licenses ,Benefits, Distribution (social service) ,Employee authentication ,Military programs

Commercial

Banking and financial services represent enormous growth areas for biometric technology, with many deployments currently functioning and pilot project announced frequently. Some

applications in this sector are: Account access, ATMs, Expanded Service Kiosks, Online banking, Telephony transaction, PC/Network access, Physical access, E-commerce, Time and attendance monitoring

Health Care

The applications in this sector includes the use of biometrics to identify or verify the identity of individuals interacting with a health-care entity or acting in the capacity of health-care employee or professional. The main aim of biometrics is to prevent fraud, protect the patient information and control the sell of pharmaceutical products. Some typical application are:PC/Network Access, Access to personal information, Patient identification

Travel and Immigration

The application in this sector includes the use of biometrics to identify or verify the identity of individual interacting during the course of travel, with a travel or immigration entity or acting in the capacity of travel or immigration employee. Typical application are: Air travel, Border crossing, Employee access,Passports (xxxvi).

Biometrics can be used for both steps, identification requiring a one-to-many search in the templates database and authentication a one-to-one comparisonof the measured biometric with the template that is associated to the claimed identity.There exist three types of authentication factors: something you know (e.g. password), something you have (e.g. token device, badge) and something you are. Biometrics fall in the third category, which is by definition the most secure because most companies still struggle to implement good password practices and when token devices or badge readers are used they get lost or are shared among colleagues([xxxvii]).

As in this figure :

something you know (e.g. password)

↓

something you have (e.g. token device, badge)

↓

something you are

* Biometric Time Clocks or Biometric time and attendance systems, which are being increasingly used in various organizations to control employee timekeeping.



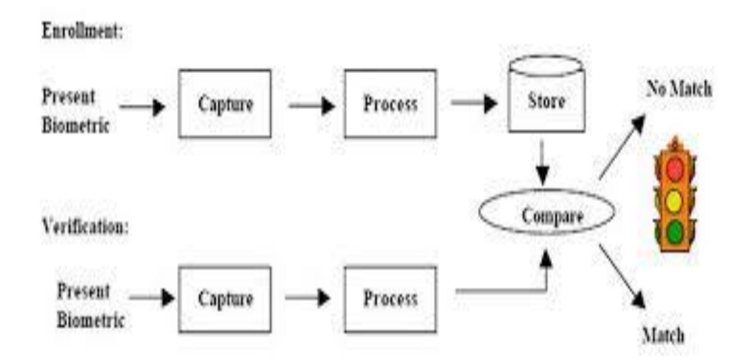
* Biometric safes and biometric locks, provides security to the homeowners.



* Biometric access control systems, providing strong security at entrances.



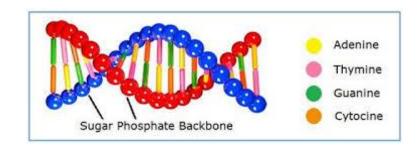
* Biometric systems are also developed for securing access to pc's and providing single logon facilities.



* Wireless biometrics for high end security and providing safer transactions from wireless devices like PDA's, etc.



* Applications of biometrics technology in identifying DNA patterns for identifying criminals, etc.



* Biometrics airport security devices are also deployed at some of the world's famous airports to enhance thesecurity standards(xxxviii).

In addition to other current and future applications that will be used broadly in biometrics:

Access control



Obtaining access to a secured area or system is mostly a two-step process:

Identification,the process by which the user professes an identity by providing a username, a pincode or some other form of ID.

Authentication, the process of verification or testing to make sure that the user is who he claims to be.([xxxix])

Biometric Access Control - How it works?

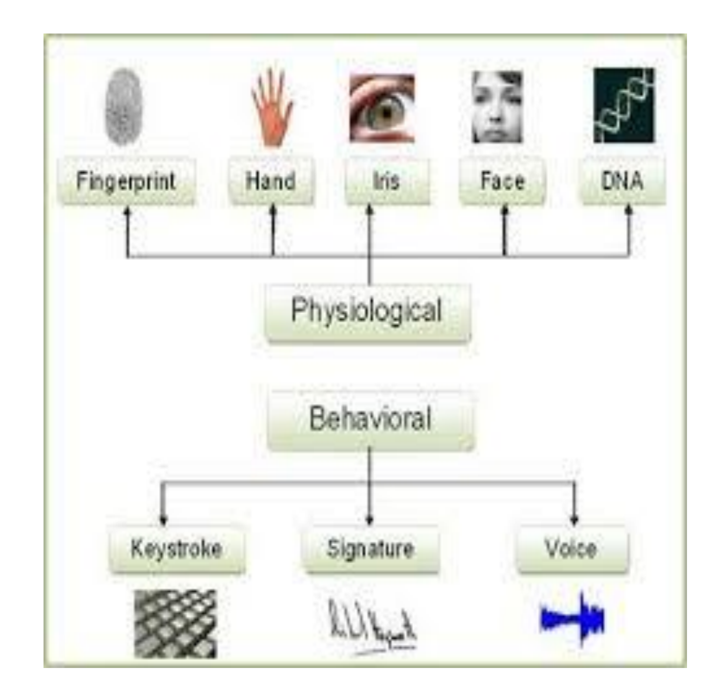
Control Panel
Access Control Server
Database
ID Credential
Reader
Software
Head-end System
Door Lock
Additional Control Panels
ID Credential
Reader
Architecture of Access Control System
Door Lock

Biometric Access Control Systems : An Overview([xl])

Any biometric access control system will consists of a biometric access control reader or scanner. This is the unit which captures the raw data in the form of fingerprint or information from iris scan, etc. This data is then analyzed & compared to the person's characteristics against the previously enrolled record. If the two records match, the person is authenticated. And if the time is within the authorized period for entry, the device will signal & release the electric door lock. The most common aspect of biometrics being used for access control is fingerprints. Though in more secure areas like defense areas and airports, government areas, etc. iris scanning systems, and other hitech approaches are being used. The best solution for a small business is to opt for a fingerprint access control system. Click here to know more about I Guard: Fingerprint Access Control System(xli).

Types of Biometrics:

There are two categories of biometrics as we have mentioned before: physiological and behavioral. Indeed, there are many studies that handled these types of biometrics like) ([xlvii]) ([xlvi])([xlv]) ([xliv])([xliii])،([xlii]and the researcher will deal with each one briefly:



DNA Matching

Chemical Biometric The identification of an individual using the analysis of segments from DNA.

Ear

Visual Biometric The identification of an individual using the shape of the ear.

Eyes - Iris Recognition

Visual Biometric The use of the features found in the iris to identify an individual.

Eyes - Retina Recognition

Visual Biometric The use of patterns of veins in the back of the eye to accomplish recognition.

Face Recognition

Visual Biometric The analysis of facial features or patterns for the authentication or recognition of an individuals identity. Most face recognition systems either use eigenfaces or local feature analysis.

Fingerprint Recognition

Visual Biometric The use of the ridges and valleys (minutiae) found on the surface tips of a human finger to identify an individual.

Finger Geometry Recognition

Visual/Spatial Biometric The use of 3D geometry of the finger to determine identity.

Gait

Behavioural Biometric The use of an individuals walking style or gait to determine identity.

Hand Geometry Recognition

Visual/Spatial Biometric The use of the geometric features of the hand such as the lengths of fingers and thewidth of the hand to identify an individual.

Odour

Olfactory Biometric The use of an individuals odor to determine identity.

Signature Recognition

Visual/Behavioral Biometric The authentication of an individual by the analysis of handwriting style, in particular the signature. There are two key types of digital handwritten signature authentication, Static and Dynamic. Static is most often a visual comparison between one scanned signature and another scanned signature, or a scanned signature against an ink signature. Technology is available to check two scanned signatures using advances algorithms. Dynamic is becoming more popular as ceremony data is captured along with the X,Y,T and P Coordinates of the signor from the signing device. This data can be utilised in a court of law using digital forensic examination tools, and to create a biometric template from which dynamic signatures can be authenticated either at time of signing or post signing, and as triggers in workflow processes.

Typing Recognition

Behavioural Biometric The use of the unique characteristics of a persons typing for establishing identity.

Vein Recognition

Vein recognition is a type of biometrics that can be used to identify individuals based on the vein patterns in the human finger or palm.

Voice / Speaker Recognition

There are two major applications of speaker recognition:

Voice - Speaker Verification / Authentication

Auditory Biometric The use of the voice as a method of determining the identity of a speaker for access control.

If the speaker claims to be of a certain identity and the voice is used to verify this claim. Speaker verification is a 1:1 match where one speaker's voice is matched to one template (also called a "voice print" or "voice model"). Speaker verification is usually employed as a "gatekeeper" in order to provide access to a secure system (e.g.: telephone banking). These systems operate with the user's knowledge and typically require their cooperation.

For example, presenting a person's passport at border control is a verification process - the agent compares the person's face to the picture in the document.

Voice - Speaker Identification

Auditory Biometric Identification is the task of determining an unknown speaker's identity.

Speaker identification is a 1:N (many) match where the voice is compared against N templates. Speaker identification systems can also be implemented covertly without the user's knowledge to identify talkers in a discussion, alert automated systems of speaker changes, check if a user is already enrolled in a system, etc..

To draw a comparison among all these types of Biometrics is a very important objective the present study seeks to achieve. For Jain, Ross and Prabakar, they states seven factors:Universality, distinctiveness, permanence, collectability, performance, acceptability, and circumvention.

As indicated in the following table: biometrics characteristics and systems :

Table 1 – Comparison of Various Biometric Technologies
(H = High, M = Medium and L = Low)

Biometric identifier	Universality	Distinctiveness	Permanence	Collectability	Performance	Acceptability	Circumvention
DNA	H	H	H	L	H	L	L
Ear	M	M	H	M	M	H	M
Face	H	L	M	H	L	H	H
Facial thermogram	H	H	L	H	M	H	L
Fingerprint	M	H	H	M	H	M	M
Gait	M	L	L	H	L	H	M
Hand geometry	M	M	M	H	M	M	M
Hand vein	M	M	M	M	M	M	L
Iris	H	H	H	M	H	L	L
Keystroke	L	L	L	M	L	M	M
Odor	H	H	H	L	L	M	L
Palmprint	M	H	H	M	H	M	M
Retina	H	H	M	L	H	L	L
Signature	L	L	L	H	L	H	H
Voice	M	L	L	M	L	H	H

Source: Anil K. Jain, Arun Ross, and Salil Prabhakar, "An Introduction to Biometric Recognition," *IEEE Transactions on Circuits and Systems for Video Technology*, Vol. 14, No. 1, January 2004.

Use of Biometrics in Libraries and Information Sciences

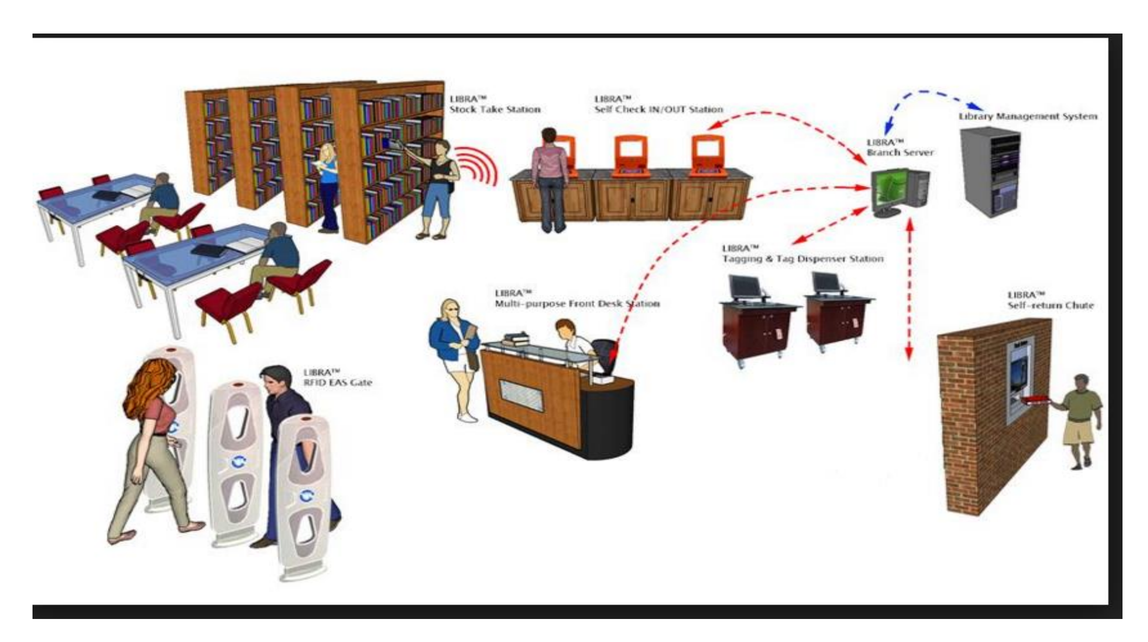
It is assumed that biometrics applications are used only in the last previous mentioned sectors, but biometrics are used in a considerable number of sectors like airports ,commercial dealings , forensic medicine ,and schools in 2012.The Information Commissioner's Office (ICO) stated that "such an enterprise should only beintroduced when explicitly authorized by the Government and should besubject to public debate and appropriate legislation."Legislation was introduced, with the Protection of Freedoms Act 2012creating an explicit legal framework for the use of biometric technologies inschools for the first time. Parents and pupils were given a legal guaranteethat no finger prints would be taken without explicit consent being obtainedfirst and that an alternative must be made available if they did not wish to
use a biometric system([xlviii]).



From the researcher's point of view, using biometrics applications in schools have paved the way for biometrics to be used in libraries and information centers securely. As libraries one of the most vital places that need to be secured, they are attacked by hackers'art of their users however they must provide researchers and students with all information at the present.

Consequently, this study sheds light on using biometrics in Academic Libraries as an existing entity. While using biometrics in Digital libraries that depend on networks and systems is very fruitful for users to log in their accounts instead of using their passwords and this what the researcher seeks to achieve in her future study. The reason beyond using Biometrics in libraries instead of library cards is organize the way of access for all users and to save time. Nevertheless, using biometrics can solve all librarians' problems in checking users' identity.

The library at an educational organization is a natural fit for adopting a biometric solution. Keeping track of a user and their activity of the library's resources not only provides a high level of security, but also on a day-to-day basis, the library can operate quicker and more efficiently. It's a good gateway for testing a system in a closed environment, before then introducing biometric controls to other services and departments ([xlix]).



<http://www.hkc.com.hk/newsletter/201209/eng/>

Hong, L., Jain, A. K., &Pankanti highlight the main applicatons of biometrics in libraries easily. The Biometric System may easily be applicable to Library System Management in three ways: a) it maintains library patron records very quickly, accurately, orderly; b) it acts as a helpful management Tool for the librarian and other managerial staff of the library; and c) it may continue for years together without any further adding cost after its installation(l)

The following figure shows that Biometrics is based patron authentication system can easily be Introduced in the library management system, which resulting the full proof security cum automated library System. A fingerprint-based door locks & hand geometry verification system.(li)



Source : Library Management System using RFID([lii])

Using of Biometrics in Academic Libraries:

- **Controlled Access to Library Premises**

This type of biometric application will not allow any unauthorized person to open the door. In this application, fingerprints of the authorized users will be scanned and stored for verification. This fingerprint identification is really a secure, convenient, and cost-effective alternative to passwords, badges, swipe cards and PINs. The biometric reader mounts on a wall near the library main door.([liii]).

Each and every library has a manual gate checking system. At least two persons are engaged for doing this job. If biometric system is introduced in the library, it should be fixed with the entrance gate of the library. The authorized library members and library staff members would be able to open the gate by themselves. Non-members should have the assistance to enter the library([liv])

These biometric fingerprint scanners offer various levels of authorization for an individual. This authorization includes a scheduling mechanism for allowing access for individuals based on the time of day. This can be applied for the whole library or at least for the computer rooms and server/ network stations to avoid unauthorized access ([lv])

- **Closed Circuit Television**

Use of CCTV cameras and biometric methods for surveillance in libraries to safe guard its possession of books and information. This paper presents the various types of CCTV cameras, their functioning and uses. A brief discussion of biometric methods like fingerprint scanning, iris scanning, facial recognition, voice recognition and palm vein authentication is presented. Finally the author recommends that the libraries in India should initiate the implementation of biometric methods and surveillance of the libraries by using CCTV cameras([lvi]).

The factors that must be considered a when using Biometric Technologies:

Biometrics is not a panacea. Implementation should be the result of cost/benefit analysis stemming from a risk assessment. However, regulatory constraints sometimes make our decision easy. The only thing possible at that point is to select the solution that makes sense([lvii])

Before deciding to use Biometric Technologies in libraries must officials before the application of biometrics taking into consideration the following:

.1#Conduct an audit of your current infrastructure

Before deciding on which biometric system to implement at your business, it will be important to conduct an audit of your existing security infrastructure, and see how well it matches up against your current security policies. Conducting a security audit will give you the chance to know and better understand your current business processes.

.2#Which biometric modality is best for your business?

There is no "one size fits all" strategy, when it comes to implementing biometrics in any business. Every business should consider some related factors when choosing a biometric modality. The most commonly implemented biometric modalities include: Fingerprint, facial recognition, iris, palm vein, and finger vein.

Factors that must be taken into account when implementing a biometric system include, but are not limited to: physical location, security risks, task (identification or verification), expected number of end users, user circumstances, and existing data.

Each biometric modality has its own strengths and weaknesses that must be evaluated in relation to the application before implementation. The effectiveness of a particular biometric system deployment is dependent on how and where the technology is used.

.3#Multimodal Biometric VsUnimodal Biometric Systems

One of the most important rules of a good security policy is to never rely upon one means of security as your only line of defense. Instead, it is smarter to have multiple layers of security. In biometric terms, this means having a multimodal biometric system for your business. Before you implement your biometric system, it is very important to see how well you can implement it alongside with your existing security systems.

A unimodal biometric system captures and matches only one biometric trait resulting in an absence of sustainable ways to solve identification problems. Some of the limitations imposed by unimodal biometric systems can be overcome by using multiple biometric modalities. Such systems, known as multimodal biometric systems, are expected to be more reliable due to the presence of multiple, independent biometric traits. A good example of a multimodal biometric solution would be Hybrid Biometric Platform™. Hybrid Biometric Platform is a multimodal biometrics system that supports any form of biometrics, including fingerprint, finger vein, palm vein, iris, and facial recognition.

.4#Biometric Hardware

With rapid innovations in biometric technology, various types of hardware are now available to choose from. Businesses need to consider all related hardware factors that may have an effect on the success of the deployment such as: liveness detection capability, spoof detection capability, and mobility. There are now smart fingerprint readers available in the market such as M2-FuseID™, which is capable of capturing a high-quality fingerprint image as well as finger vein pattern for liveness detection and to eliminate spoof attacks.

5#Consider the ROI

If you have already decided that you want to implement a biometric system, it is important that you develop an understanding for the rate of Return on Investment (ROI). In order to understand this, you can first conduct a "Pilot Project". For example, if your implementation calls for the deployment of five fingerprint scanners at five different points for employee time and attendance tracking at your place of business, first consider deploying only one fingerprint scanner at one primary point for a short period of time. By doing this, you can then quantify your ROI if you want to do a system wide deployment. Also, this will give you time to see how your employees will react to the use of a biometric system. You can always implement a system wide biometric deployment, but you run the risk of not knowing what your ROI will be, as well as your employee's perception and acceptance of the new technology.([lviii])

ARVIND MUTHUKRISHNAN adds thatBefore choosing a biometrics user authentication solution, an organization should evaluate its needs carefully. The following list includes items that should be considered the order of importance depends on the environment and level of security needed.

- **Level of security required**
- **Accuracy**
- **Cost and Implementation time**
- **User acceptance([lix])**

Advantages of using biometrics in Libraries:

In the following points, we propose advantages of using biometrics in Academic Libraries:

Biometric traits cannot be lost or forgotten while passwords can be lost or forgotten.

- Biometric traits are difficult to copy, share and distribute. Passwords can be announced in cracker's websites.
- Biometrics require the person being authenticated to be present at the time and point of authentication.
- The systems are easy to manage and cost efficient
- It is convenient to the users as they no longer responsible for passwords, swipe or proximity cards, PINs or keys.([lx])
- Recurring cost for Library card eliminated
- Easy and foolproof verification of end user
- Rack management for book retrieval
- Dynamic & easy searching of books
- Online budget and account maintenance
- Instant reports
- No misuse of authority
- Full inventory control ([lxi])

Defects of Using Biometrics:

- Though the biometrics technology provides a number of advantages, there are some disadvantages
- Too. The following are a select list of problems associated with the system.
- Biometric technology is inherently individuating and interfaces easily to database technology,
- Making privacy violations easier and more damaging.
- Biometric systems are useless without a well-considered threat model.
- Biometrics are no substitute for quality data about potential risks.
- Biometric identification is only as good as the initial ID.
- Some biometric technologies are discriminatory.
- Biometric systems' accuracy is impossible to assess before deployment
- The cost of failure is high ([lxii]).

Conclusion:

Finally, the present paper ends with a conclusion, which summarizes all research findings. Moreover, the researcher, hence, proposes further topics for future studies, as a result of his thesis' findings. For biometrics and their use in Academic Libraries, the researcher can proposea number of recommended topics for futurestudies asfollow?

* No fixed biometric system is better than other systems.

* Academic Librariesshouldchoose for themselves the best biometric system where biometrics vary in cost and suitability for different applications.

*Librarians should learn how to use biometrics applications.

*Informingbeneficiaries of what will be done with the data stored and their (properties).

*Educating current and future users of the benefits of biometrics technology in order to ensure its effectiveness.

*Raising awareness of Biometrics in academic circlesand their acceptance and effectiveness to facilitate work in Academic Libraries.

References

(i) Gates, Kelly Allison Our Biometric Future: The Social Construction of an Emerging Information Technology.- Thesis (Ph.D.)--University of Illinois at Urbana-Champaign, 2004.**Access date (10/2/2016).- Available on:http://hdl.handle.net/2142/86567**

(2)Forkin, M. (2011). ***Ocular biometrics: Human recognition in challenging conditions*** (Order No. 1494561). Available from ProQuest Dissertations & Theses Global. (874642298). Access date (15/2/2016).- Available on:

http://search.proquest.com/docview/874642298?accountid=37552

(iii)Nwatu, G. U. (2011). *Biometrics technology: Understanding dynamics influencing adoption for control of identification deception within nigeria* (Order No. 3461683). Available from ProQuest Dissertations & Theses Global. (881755664). Access date (10/2/2016).- Available on:http://search.proquest.com/docview/881755664?accountid=37552

(iv**)** (Yampolskiy, R. V. (2008). *Intrusion detection using spatial information and behavioral biometrics* . State University of New York at Buffalo Buffalo, NY, USA (Order No. 3320379). Available from ProQuest Dissertations & Theses Global. (304373064). Access date (10/2/2016).- Available on:http://search.proquest.com/docview/304373064?accountid=37552

(v)Gan, W. (2007). *A statistical approach towards performance analysis of multimodal biometrics systems* ," *Robotics and Biomimetics,. ROBIO 2008. IEEE International Conference on*, Bangkok, 2009, pp. 877-882. doi: 10.1109/ROBIO.2009.4913115 Access date (25/1/2016).- Available on:

URL: http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=4913115&isnumber=4912969

(vi) Ma, Y. (2007). *An empirical investigation of tree ensembles in biometrics and bioinformatics research* (Order No. 3298557).Available from ProQuest Dissertations & Theses Global. (304815103). Access date (10/2/2016).- Available on:http://search.proquest.com/docview/304815103?accountid=37552

(vii)Guzman Tamayo, Ana M., "Thermal Imaging As A Biometrics Approach To Facial Signature Authentication" (2011). FIU Electronic Theses and Dissertations.Paper 539.http://digitalcommons.fiu.edu/etd/539Access date (10/2/2016).- Available on:

http://digitalcommons.fiu.edu/cgi/viewcontent.cgi?article=1635&context=etd

(viii) Mohamed,OmarHamdy(2010). HOMOGENEOUS COGNITIVE BASED BIOMETRICS FOR STATIC AUTHENTICATIONAccess date (30/2/2016).- Available on:

https://dspace.library.uvic.ca/bitstream/handle/1828/3211/Mohamed_Omar_PhD_2010.pdf?sequence=1

(ix)Brydie, D. R. (2009). *Situational considerations in information security: Factors influencing perceived invasiveness toward biometrics* (Order No. 3339284). Available from ProQuest Dissertations & Theses Global. (288100321). Access date (30/1/2016).- Available on:http://search.proquest.com/docview/288100321?accountid=37552

(x)MehrbanyIrany, B. (2011). *A high capacity reversible multiple watermarking scheme - applications to images, medical data, and biometrics* Access date (13/2/2016).- Available on: https://tspace.library.utoronto.ca/bitstream/1807/29530/6/MehrbanyIrany_Behrang_201106_MASc_thesis.pdf

(xi) Ravinder Singh Gulair, Karan Sheth Overview of BiometricsTechno-Innova 2004. Access date (13/2/2016).- Available on:

http://www.oocities.org/slazetech/Biometrics.pdf

(xii) Ibid

(xiii) MariosSavvides .Introduction to Biometric Recognition Technologies and Applications.Access date (13/2/2016).- Available on:

https://users.ece.cmu.edu/~jzhu/class/18200/F05/Lecture06_Marios_Lecture.pdf

(xiv) Norman Desmarais, (2000) "Body language, security and e-commerce", Library Hi Tech, Vol. 18 Iss: 1, pp.61 – 74Access date (21/2/2016).- Available on:

http://www.emeraldinsight.com.ugrade1.eul.edu.eg:2048/doi/full/10.1108/07378830010314483

(xv) Op.cit

(xvi) Op.cit

(xvii) Biometric Technology An introduction to the science (as applied to DL/ID requirements) Ian Williams Principal. Access date (30/2/2016).- Available on:

www.idsysgroup.comhttp://www.idsysgroup.com/ftp/biometrics_101_ISG.pdf

(xviii) Siddhesh Angle, ReemaBhagtani, HemaliChheda .2006 . BIOMETRICS : A FURTHER ECHELON OF SECURITY .- Journal of Organizational and End User Computing, vol. 18, no. 3
(xix)Op.cit

(xx) Biometrics.. Access date (9/2/2016).- Available on:

http://www.merriam-webster.com/dictionary/biometrics

(xxi)biometrics. (n.d.). *Dictionary.com Unabridged*. from Dictionary.com websiteAccess date (9/2/2016).- Available on: http://www.dictionary.com/browse/biometrics

(xxii)Op.cit

(xxiii)Definition of biometrics. The International Biometric Society. Access date (13/2/2016).- Available on: http://www.biometricsociety.org/about/definition-of-biometrics/
(xxiv) Joan M. Reitz.ODLIS: Online Dictionary for Library and InformationScience. Access date (9/2/2016).- Available on: http://www.abc-clio.com/ODLIS/odlis_b.aspx

(xxv) Biometrics and Your Library.Blog of a section of an introduction to the library profession course. JUNE 11, 2009Access date (17/3/2016).- Available on:

HTTP://LIS6010BLOG.BLOGSPOT.COM.EG/2009/06/BIOMETRICS-AND-YOUR-LIBRARY.HTML
(xxvi)Christensson, P. (2012, January 30). *Biometrics Definition*.Access date (7/1/2016).- Available on: http://techterms.com

(xxvii) *Aleksandra Babich (2012)Biometric Authentication. Types of biometric identifiers.- Bachelor's Thesis Degree Programme in Business Information Technology* ***Access date (17/3/2016).- Available on:***
https://www.theseus.fi/bitstream/handle/10024/44684/Babich_Aleksandra.pdf?sequence=1
(xxviii)*Op.cit*
(xxix) HISTORY OF BIOMETRICS Access date (17/3/2016).- Available on:

http://ntrg.cs.tcd.ie/undergrad/4ba2.02/biometrics/history.html

(xxx) LAUREN KATIMS NADEAU (2012).Tracing the History of Biometrics.*The practice of distinguishing humans based on intrinsic physical or behavior traits goes back thousands of years.* Access date 15/1/2016).- Available on:

http://www.govtech.com/Tracing-the-History-of-Biometrics.html

) xxxi(G Rathinasabapathy T MohanaSundariThiru L Rajendran.(2008). Biometric Applications in Library and Information Centres:Prospects and Problems..International CALIBER-. Access date 15/1/2016).- Available on:

.https://www.researchgate.net/publication/256462798

Available on: -)Biometric Applications . Access date 15/1/2016).xxxii(
http://www.griaulebiometrics.com/en-us/book/understanding-

biometrics/introduction/applications-2

(xxxiii)***Applications of Biometrics*** : Areas harnessing the technology.Access date(19/1/2016).- Available on:http://www.questbiometrics.com/applications-of-biometrics.html

(xxxiv) Biometric Recognition: Security and Privacy ConcernsAccess date 16/3/2016).- Available on:

http://biometrics.cse.msu.edu/Publications/GeneralBiometrics/PrabhakarPankantiJain_BiometricSecurityPrivacy_SPM03.pdf

(xxxv) http://www.fujitsu.com/global/about/resources/news/press-releases/2011/0601-01.html

)xxxvi(Op.cit

) xxxvii(Biometric ApplicationsAccess date (17/3/2016).- Available on:

http://www.biometric-solutions.com/applications/index.php

(xxxviii)*Op.cit*

Op.cit)**(xxxix**

(xl)<http://www.questbiometrics.com/biometric-access-control.html>

(xli)Biometric Access Control Systems : An Overview. Access date (17/3/2016).- Available on:

http://www.questbiometrics.com/biometric-access-control.html

(xlii) Types of Biometrics.-The Biometrics Institute. Access date (13/2/2016).- Available on:http://www.biometricsinstitute.org/pages/types-of-biometrics.html

(xliii)Op.cit

(xliv) Sheila Robinson (2011)Using Biometry for Security and Identification.Access date (13/2/2016).- Available on:http://www.brighthub.com/computing/smb-security/articles/63325.aspx

(xlv) **K P Tripathi**.(2011) **A Comparative Study of Biometric Technologies with Reference to Human Interface.-** International Journal of Computer Applications (0975 – 8887) Volume 14– No.5 Access date(17/3/2016).-Available on http://www.ijcaonline.org/volume14/number5/pxc3872493.pdf

(xlvi) Biometrics in Schools The extent of Biometrics in English secondary schools and academies .2014 Access date (13/2/2016).- Available on: https://www.bigbrotherwatch.org.uk/files/reports/Biometrics_final.pdf

(xlix) http://biostore.co.uk/company/news-articles/biometrics-secure-access-to-library-resources/

(l) Hong, L., Jain, A. K., &Pankanti, S.(1999) "Can Multibiometrics Improve Performance?", Proc. AutoID'99, pp. 59-64, Summit(NJ), USA,

(li): Library Management System using RFID. Access date (17/3/2016).- Available on:.http://www.rfid-library.com/

(lii) http://www.rfid-library.com/
(liii) Op.cit

(liv) **M. R. Ramesh** (2012 **Biometric Recognition: A New Approach for Library Patron Authentication.-**) International Journal of Library Science 2012, 1(5): 72-74 DOI: 10.5923/j.library.20120105.01
(lvOp.cit

(lvi) Y V RAMANA(2007). SECURITY IN LIBRARIES NEED SURVEILLANCE AND BIOMETRICS 5th International CALIBER -2007, Panjab University, Chandigarh, Access date (8/3/2016).- Available on:http://ir.inflibnet.ac.in/bitstream/1944/1427/1/498-507.pdf
(lvii) Tom Olzak .(2012).Applications of Biometrics.- **Access date (11/1/2016).- Available on:.** *http://resources.infosecinstitute.com/chapter-12-applications-of-biometrics/*
(lviii) Mohammad Shahnewaz.2015. *5 Things to Consider Before Deploying a Biometric System for Your Business.- M2SYS Blog On Biometric Technology* **.- Access date (20/3/2016).- Available on:.** http://blog.m2sys.com/workforce-management/5-things-to-consider-before-deploying-a-biometric-system-for-your-business/
(lix) Muthukrishnan'sArvind .(2009). Basics of Biometrics for beginners.- ArvindMuthukrishnan's Blog.- Access date (12/1/2016).- Available on:. http://arvindmuthukrishnan.blogspot.com.eg/

(lx)Panneerselvam, Selvi, M. G.(2007) Biometrics: libraries have begun to see the value of biometrics.,. In National Conference on Future Technologies for Empowering LIS Professisonal: Challenges and Opportunities, Chennai, India, 9-11 August 2007. [Presentation] .- Access date (16/3/2016).- Available on:. http://hdl.handle.net/10760/11759